Listing of Claims

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

defining a key and a set of values, the key able to be derived using the values and a predefined relationship between the values;

sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage; and

sending a second value of the set, but not all of the values of the set to a first delegate,

wherein the first delegate comprises a person or an entity who has been authorized to access the encrypted information, and

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values of the set absent the second of the values of the set, and

inaccessible with the second of the values of the set absent the first of the values of the set.

2. (Previously Presented) The method of claim 1 further comprising:

generating a second set of values, the key being determinable by the values of the second set;

sending a first but not all of the values of the second set to the server; and

sending a second but not all of the values of the second set to a second delegate,

wherein the encrypted information is

inaccessible with the first of the values of the second set absent the second of the values of the second set, and

inaccessible with the second of the values of the second set absent the first of the values of the second set.

3. (Previously Presented) The method of claim 2 in which the values of the second set are also determinable by the predefined relationship.

4. (Original) The method of claim 1 in which the set includes exactly two values.

5. (Original) The method of claim 1 in which the set includes three or more values.

6. (Previously Presented) The method of claim 1 in which the first value is associated with a descriptor of the first delegate.

7. (Previously Presented) The method of claim 1 in which the probability of guessing the key correctly using knowledge of one or more of the values of the set, but not all the values of the set, is the same as the probability of guessing the key correctly using no knowledge of any value of the set.

8. (Previously Presented) The method of claim 7 in which the predefined relationship comprises one or more of the Boolean XOR function and a relationship that applies an encryption algorithm to one value of the set using another value of the set as the encryption algorithm key.

9. (Original) The method of claim 1 in which the information comprises medical information.

10. (Currently Amended) A method comprising:

storing, on a server accessible through a network, secured information and a first access component, access to the secured information requiring a key, the key able to be derived using the first access component, a second access component, and a relationship between the first and second access components;

excluding both the key and the second access component from storage on the server; and

providing the secured information and the first access component to a first requestor, wherein the first requestor comprises a delegate who has been authorized to access the secured information.

11. (Canceled)

12. (Previously Presented) The method of claim 10 further comprising storing a third access component on the server, the third access component, when combined with a fourth access component that is excluded from storage on the server, being sufficient to permit access to the secured information.

13. (Original) The method of claim 12 further comprising providing the secured information and the third access component to a second requestor.

14. (Original) The method of claim 12 further comprising deleting the third access component in response to a trigger, the trigger being a client instruction, a time limit, a request from the first requestor, or a security breach.

15. (Original) The method of claim 12 further comprising identifying the requestor and determining that the requestor requires the first access component but not the third access component.

16. (Previously Presented) The method of claim 10 further comprising storing permission information about a party approved for access, such that the secured information and the first access component are only provided if the first requestor is the approved party.

17. (Original) The method of claim 10 in which the secured information is secured by encryption using a key, and the first and second access components are related to the key by a predefined relationship.

18. (Previously Presented) A method comprising:

receiving

a) from a client, a first access component,

b) from a server accessible through a network, secured information, access to the secured information requiring a key, the key able to be derived using the first access component and a second access component, and

c) from a source other than the client or the server, the second access component,

wherein the secured information is

accessible with the key,

inaccessible with the first access component absent the second access component, and

inaccessible with the second access component absent the first access component.

19. (Original) The method of claim 18 in which the source is the server.

20. (Canceled)

21. (Original) The method of claim 18 in which a third access component is required in addition to the first and second access components for use of the secured information.

22. (Original) The method of claim 18 in which the secured information, the first access component, and the second access component are received in a digital form.

23. (Currently Amended) An article comprising a machine-readable medium that stores machine-executable instructions, the instructions being operable to cause a machine to:

define a key and a set of values, the key able to be derived using the values and a predefined relationship between the values;

send a first but not all of the values of the set and information encrypted using the key to a server for storage; and

send a second but not all of the values of the set to a first delegate,

wherein the first delegate comprises a person or an entity who has been authorized by a definer of the key and the set of values to access the encrypted information, and

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values absent the second of the values, and

inaccessible with the second of the values absent the first of the values.

24. (Previously Presented) The article of claim 23 in which the instructions further cause a machine to:

generate a second set of values, the key being independently determinable by the values of the second set;

send a first but not all of the values of the second set to the server; and

send a second but not all of the values of the second set to a second delegate,

wherein the encrypted information is

inaccessible with the first of the values of the second set absent the second of the values of the second set, and

inaccessible with the second of the values of the second set absent the first of the values of the second set.

25. (Currently Amended) An apparatus comprising a processor and instructions configured to cause the processor to:

receive, from a client, information and a value of a set of values, the information being encrypted using a key, the key able to be derived using the values of the set and a predefined relationship between the values;

store the information and the value, but not all the values of the set; and

transmit, to a delegate who has been authorized by the client to access the information, the information and the value.

26. (Original) The apparatus of claim 25 in which the software is further configured to cause the processor to:

store a second value that is a member of a second set of values, the values of the second set being sufficient to determine the key using the predefined relationship.

27. (Previously Presented) The apparatus of claim 26 in which the software is further configured to cause the processor to:

delete or deny access to the second value in response to a trigger, the trigger being a client instruction, a time limit, a request from the delegate, or a security breach.

28. (Original) The apparatus of claim 25 in which the information comprises medical information.

Claims 29-30. (Canceled)

31. (Previously Presented) The method of claim 1 further comprising sending, to the server, instructions for allowing the first delegate to access the first of the values.

32. (Previously Presented) The method of claim 18, further comprising sending authentication information to the source other than the client or the server to access the second access component.

33. (Canceled)

34. (Previously Presented) The method of claim 1, wherein the person or the entity has been authorized by a definer of the key and the set of values.

35. (Canceled)

36. (Previously Presented) The method of claim 18, wherein receiving the second access component comprises receiving the second access component from a delegate who has been authorized by the client to access the secured information.

37. (Canceled)

38. (Canceled)

39. (New) A method comprising:

defining a key and a set of values, the key able to be derived using the values and a predefined relationship between the values;

sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage;

sending a second value of the set, but not all of the values of the set to a first delegate;

generating a second set of values, the key being determinable by the values of the second set;

sending a first but not all of the values of the second set to the server; and

sending a second but not all of the values of the second set to a second delegate,

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values of the set absent the second of the values of the set,

inaccessible with the second of the values of the set absent the first of the values of the set,

inaccessible with the first of the values of the second set absent the second of the values of the second set, and

inaccessible with the second of the values of the second set absent the first of the values of the second set.

40. (New) The method of claim 39 in which the values of the second set are also determinable by the predefined relationship.

41. (New) The method of claim 39 in which the first value is associated with a descriptor of the first delegate.

42. (New) A method comprising:

defining a key and a set of three or more values, the key able to be derived using the values and a predefined relationship between the values;

sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage; and

sending a second value of the set, but not all of the values of the set to a first delegate,

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values of the set absent the second of the values of the set, and

inaccessible with the second of the values of the set absent the first of the values of the set.

43. (New) A method comprising:

defining a key and a set of values, the key able to be derived using the values and a predefined relationship between the values;

sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage; and

sending a second value of the set, but not all of the values of the set to a first delegate,

wherein the first value is associated with a descriptor of the first delegate, and

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values of the set absent the second of the values of the set, and

inaccessible with the second of the values of the set absent the first of the values of the set.

44. (New) A method comprising:

defining a key and a set of values, the key able to be derived using the values and a predefined relationship between the values;

sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage; and

sending a second value of the set, but not all of the values of the set to a first delegate,

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values of the set absent the second of the values of the set, and

inaccessible with the second of the values of the set absent the first of the values of the set, and

wherein the probability of guessing the key correctly using knowledge of one or more of the values of the set, but not all the values of the set, is the same as the probability of guessing the key correctly using no knowledge of any value of the set.

45. (New) The method of claim 44 in which the predefined relationship comprises one or more of the Boolean XOR function and a relationship that applies an encryption algorithm to one value of the set using another value of the set as the encryption algorithm key.

46. (New) A method comprising:

storing, on a server accessible through a network, secured information and a first access component, access to the secured information requiring a key, the key able to be derived using the first access component, a second access component, and a relationship between the first and second access components;

excluding both the key and the second access component from storage on the server;

storing a third access component on the server, the third access component, when combined with a fourth access component that is excluded from storage on the server, being sufficient to permit access to the secured information; and

providing the secured information and the first access component to a first requestor.

47. (New) The method of claim 46 further comprising providing the secured information and the third access component to a second requestor.

48. (New) The method of claim 46 further comprising deleting the third access component in response to a trigger, the trigger being a client instruction, a time limit, a request from the first requestor, or a security breach.

49. (New) The method of claim 46 further comprising identifying the requestor and determining that the requestor requires the first access component but not the third access component.

50. (New) The method of claim 46 further comprising storing permission information about a party approved for access, such that the secured information and the first access component are only provided if the first requestor is the approved party.

51. (New) The method of claim 46 in which the secured information is secured by encryption using a key, and the first and second access components are related to the key by a predefined relationship.

52. (New) An article comprising a machine-readable medium that stores machine-executable instructions, the instructions being cperable to cause a machine to:

define a key and a set of values, the key able to be derived using the values and a predefined relationship between the values;

send a first but not all of the values of the set and information encrypted using the key to a server for storage;

send a second but not all of the values of the set to a first delegate;

generate a second set of values, the key being independently determinable by the values of the second set;

send a first but not all of the values of the second set to the server; and

send a second but not all of the values of the second set to a second delegate,

wherein the encrypted information is

accessible with the key,

inaccessible with the first of the values absent the second of the values,

inaccessible with the second of the values absent the first of the values,

inaccessible with the first of the values of the second set absent the second of the values of the second set, and

inaccessible with the second of the values of the second set absent the first of the values of the second set.

53. (New) An apparatus comprising a processor and instructions configured to cause the processor to:

receive, from a client, information and a value of a set of values, the information being encrypted using a key, the key able to be derived using the values of the set and a predefined relationship between the values;

store the information and the value, but not all the values of the set;

transmit, to a delegate, the information and the value; and

delete or deny access to the second value in response to a trigger, the trigger being a client instruction, a time limit, a request from the delegate, or a security breach..

54. (New) An apparatus comprising a processor and instructions configured to cause the processor to:

receive, from a client, information and a value of a set of values, the information being encrypted using a key, the key able to be derived using the values of the set and a predefined relationship between the values;

store the information and the value, but not all the values of the set;

transmit, to a delegate, the information and the value; and

store a second value that is a member of a second set of values, the values of the second set being sufficient to determine the key using the predefined relationship.